September 21, 2026

The Honorable Charity R. Clark
109 State Street
Montpelier, VT 05609

Re: Proposed Rules Implementing §§ 2449f and 2449g of Act 63 (Vermont Age-Appropriate Design Code Act)

Dear Attorney General Clark:

The Computer & Communications Industry Association (CCIA) respectfully submits these comments in response to the proposed rules implementing §§ 2449f[1] and 2449g[2] of Act 63 of 2025, the Vermont Age-Appropriate Design Code Act ("VAADCA").[3] CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[4]

CCIA firmly believes that children are entitled to security and privacy online. Our members have developed settings, safeguards, and parental controls designed to tailor younger users' online experiences to their developmental needs. These include tools that allow parents to set time limits and restrict access to particular services, as well as enhanced privacy protections enabled by default for known child users.[5] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.[6]

While CCIA supports the Office of the Attorney General ("AGO's") commitment to protecting minors online, the proposed rules, if implemented, raise significant concerns. In numerous instances, the proposed rules exceed Act 63's scope, introduce novel legal standards not found in the enabling legislation, and contain inconsistencies that will frustrate compliance and undermine the very protections VAADCA seeks to provide. We respectfully urge the AGO to

---

[1] "Prohibited Data and Design Practices" (Regulations Adopted Pursuant to 9 V.S.A. § 2449f), https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449f%20Prohibited%20Data%20and%20Design%20Practices%20-%20FINAL%20DRAFT.pdf.
[2] "Age Assurance Privacy" (Regulations Adopted Pursuant to 9 V.S.A. § 2449g), https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449g%20Age%20Assurance%20Privacy%20-%20FINAL%20DRAFT.pdf.
[3] 9 V.S.A. §§ 2449a–2449h (2025), https://legislature.vermont.gov/Documents/2026/Docs/ACTS/ACT063/ACT063%20As%20Enacted.pdf.
[4] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[5] Competitive Enterprise Inst., *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated July 28, 2026).
[6] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.

revise the proposed rules to comply with Act 63, align with established legal frameworks, and preserve beneficial uses of data that serve minors' interests. CCIA therefore recommends the revisions detailed in the responses to the questionnaire below:

10. Discuss the relevant factors for assessing what constitutes design practices.

VAADCA authorizes the AGO to regulate design practices "that lead to compulsive use or subvert or impair user autonomy, decision making, or choice."[7] VAADCA further defines "compulsive use" as "the repetitive use of a covered business's service that materially disrupts one or more major life activities of a minor, including sleeping, eating, learning, reading, concentrating, communicating, or working."[8] To avoid legal inconsistency, interpretation of the phrase "subvert or impair user autonomy, decision making, or choice" should match the analogous definition of "dark pattern" in the Vermont Data Privacy and Online Surveillance Act (VDPOSA).[9] VDPOSA uses this terminology only in the consent context.[10] Accordingly, any design feature of a user interface deemed to invalidate user consent, either under VDPOSA or by the Federal Trade Commission, should constitute a "design practice" that the proposed rules may regulate. Designed aspects of online services that do not meet either of these criteria do not fall within VAADCA's scope.

By contrast, the proposed rules define "subvert or impair autonomy" as "practices that interfere with a covered minor's informed decision-making or make disengagement from a service harder."[11] This definition extends far beyond material disruption of major life activities, and contains no connection to the consent context. If this definition is not narrowed as proposed above, it will exceed VAADCA's statutory authority and conflict with the term's common understanding in the privacy context.

11. Discuss businesses to be considered 'covered businesses' for purposes of assessing what would subvert or impair user autonomy, decision making, or choice.

The definition of "covered business" should provide clear, objective criteria that allow businesses to determine whether they are subject to the VAADCA. As the term "reasonably likely to be accessed by a minor" is inherently subjective, the AGO should interpret this term to align with the standard for determining when an online service is "directed to" children under the Children's Online Privacy Protection Act of 1998 ("COPPA"),[12] as VAADCA does.[13] The FTC has already issued extensive guidance to assist businesses in making such determinations.[14]

---

[7] 9 V.S.A. § 2449f(b).
[8] § 2449a(8).
[9] § 2415a(b)(16) (2026), https://legislature.vermont.gov/Documents/2026/Docs/ACTS/ACT145/ACT145%20As%20Enacted.pdf..
[10] § 2415a(b)(7)(C)(iii).
[11] "Prohibited Data and Design Practices" (Regulations Adopted Pursuant to 9 V.S.A § 2449f), 3, https://ago.vermont.gov/sites/ago/files/2026-07/AADC%20rules/2026.07.08%20-%202449f%20Prohibited%20Data%20and%20Design%20Practices%20-%20FINAL%20DRAFT.pdf.
[12] 15 U.S.C. §§ 6501-06 (1998), https://www.law.cornell.edu/uscode/text/15/chapter-91.
[13] 9 V.S.A. § 2449a(26)(A) (2025).
[14] *See, e.g.*, 16 C.F.R. § 312.2.5, https://www.federalregister.gov/d/2025-05904/p-326.

Absent such guidance, businesses will likely be unable to determine in advance whether they must comply with the law.

12. Discuss the types of data processing or design practices that should be considered.

The proposed rules contain numerous conflicts with VAADCA regarding design practices. As noted above, the statute authorizes the AGO only to regulate design practices "that lead to compulsive use or subvert or impair user autonomy, decision making, or choice." However, the proposed data and design practices rules instead aim to regulate "any online service, product, or feature that is used by a covered minor."[15] Only a limited subset of all online services, products, and features used by minors will lead to the outcomes contemplated in VAADCA. CCIA therefore recommends revising the "Applicability" section of the proposed data and design practices rules to match the scope authorized by VAADCA.

The proposed data and design practices rules further exceed the statutory mandate by regulating data that does not qualify as "personal data" under VAADCA. VAADCA defines "personal data" as information "linked or reasonably linkable to an identified or identifiable individual,"[16] and does not regulate the processing of non-personal data. However, the proposed rules define "behavioral data" to include many types of data that are not necessarily "linked or reasonably linkable" to an individual. Online services regularly conduct aggregate analyses of the "clicks, scrolls, dwell time, viewing history, and navigation patterns" of their overall website traffic after de-identifying it. Such data is "behavioral data," but is not "personal data" and thus not within the proposed rules' scope. To avoid scoping in data beyond what the statute authorizes, CCIA recommends removing the definition of "behavioral data" from the proposed rules. If the behavioral data is also personal data, it will still fall within the rules' scope. Definitions and regulations referencing behavioral data should reference personal data instead.

The "behavioral inference" definition should be removed for similar reasons. Furthermore, the term does not appear elsewhere in the proposed rules, and is redundant given the definition of "inferred preferences," which covers substantially similar activities.

Furthermore, the "minimum duty of care" provision also lies outside the AGO's rulemaking authority. While VAADCA creates a "minimum duty of care" for covered businesses who process covered minors' data, it does not authorize the AGO to institute regulations regarding this duty.[17] Again, the AGO's rulemaking authority applies only when "design practices "lead to compulsive use or subvert or impair user autonomy, decision making, or choice," a far narrower set of circumstances. All regulations regarding the minimum duty of care should therefore be removed, as they exceed the authorized scope for the proposed rules.

Likewise, the proposed rules should remove the definition of "heightened risk of harm," as it covers features that are designed to increase minors' engagement generally. Because not all

[15] "Prohibited Data and Design Practices," *supra* note 1, at 1.
[16] 9 V.S.A. § 2449a(21).
[17] § 2449c.

features designed to increase minors' engagement impair user autonomy or choice, this definition broadens the proposed rules' scope beyond what VAADCA authorizes. Compulsive use determines whether the AGO can regulate a design practice, not attempts to increase engagement.

13. Discuss the types of digital products that should be considered in adopting any AADC rules for purposes of assessing an online service, product, or feature.

Assessments of online services, products, and features should be based on their actual knowledge of users' ages, not what they "have reason to know." VAADCA only applies to "a consumer who a covered business actually knows is a minor or labels as a minor pursuant to age assurance methods in rules adopted by the Attorney General."[18] By contrast, the proposed rules "apply where a covered business knows *or has reason to know* that a user is a covered minor,"[19] thus expanding VAADCA's scope from an actual knowledge standard to a constructive knowledge standard.

Besides exceeding statutory authority, the constructive knowledge standard undermines privacy and prevents equitable enforcement. Because no objective standard exists for determining when a controller "has reason to know" a user's age, covered services will be incentivized to verify the ages of all users to mitigate litigation risk, requiring the collection of additional sensitive information from both minors and adults. Furthermore, this standard is unworkable, leaving covered businesses without a reliable way to know if they are complying with the law. This standard creates unpredictable liability, especially if interpreted to include aggregate information about a service's user base rather than user-specific facts.[20]

14. Discuss what should qualify as an exclusion regarding the sale, delivery, or use of a physical product when assessing an online service, product, or feature.

This exclusion should cover all data reasonably necessary for the sale, delivery, or use of physical products. The proposed rules should not extend to addresses, shipping receipts, and other personal information commonly collected to facilitate sales of physical products. Likewise, the rules should not extend to any internal processing of this data or its use in models, nor should they apply to personal data entered into a physical device that will not be collected or processed online. Otherwise, routine information necessary to complete a transaction, deliver a product, provide warranty or customer support, or enable functionality of a physical device could inadvertently bring ordinary commercial activity within rules aimed at online design practices affecting minors.

[18] § 2449a(12).
[19] "Prohibited Data and Design Practices," *supra* note 1, at 1 (emphasis added).
[20] *See also* Jesse Lieberfeld, *Knowledge Standards in Online Safety and Privacy Legislation*, CCIA (Apr. 14, 2026), https://ccianet.org/articles/knowledge-standards-in-online-safety-and-privacy-legislation/.

15. Discuss the types of technical requirements that should be considered in the AADC rulemaking process.

The proposed AADC rules create technical requirements that directly contradict the statutory text. The rules prohibit ranking, selecting, or prioritizing content based on "inferred preferences,"[21] i.e. predictions made using "a covered minor's personal data, behavioral data, prior activity, interactions, or engagement patterns."[22] VAADCA, by contrast, explicitly allows covered businesses to recommend to covered minors "media with similar characteristics as the media they are currently viewing."[23] Implementing that statutory permission may necessarily require a service to draw conclusions about what media a user is likely to find relevant based on the media currently being viewed. Yet the proposed rules disallow these inferences even though VAADCA unambiguously permits them. The prohibition on using "inferred preferences" to rank, select, or prioritize content should therefore be removed so that the proposed rules comply with the statute.

16. Discuss the types of technical or design challenges that may prohibit data processing or design practices of a covered business for purposes of the AADC rulemaking.

Although the proposed rules do not explicitly mandate age verification, businesses nevertheless may need to *determine the age of all users* to ensure that they adhere to the regulations regarding minors. As explained above, this in turn requires using invasive age verification methods that force businesses to collect sensitive personal identifying information about their users.[24] Maintaining user privacy under these conditions can be enormously challenging.[25] A recent Digital Trust & Safety Partnership (DTSP) report found that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[26]

Additionally, age estimation software will sometimes classify adults as minors, or vice versa, and does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[27] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and

---

[21] "Prohibited Data and Design Practices," *supra* note 1, at 1.
[22] *Id.* at 12.
[23] 9 V.S.A. § 2449f(a)(4)(A)(iii) (2026).
[24] Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf.
[25] Kate Ruane, *CDT Files Brief in* NetChoice v. Bonta *Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[26] *Age Assurance: Guiding Principles and Best Practices*, DTSP (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[27] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* Nat'l Inst. Standards & Tech. (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.

interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA encourages the AGO to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

17. Discuss other factors that may be relevant in developing these rules in developing AADC rules.

Besides contradicting VAADCA as noted above, the proposed AADC rules raise serious First Amendment concerns. In 2024, the Supreme Court held in *Moody v. NetChoice LLC* that "regulating the content-moderation policies" of websites "to change the speech that will be displayed there… is a preference" that states "may not impose."[28] However, the proposed AADC rules explicitly regulate such policies to change what speech covered businesses will display. By restricting the methods through which covered services may select, rank, and present protected expression to users, the proposed rules burden editorial choices concerning the presentation of speech and therefore raise serious First Amendment concerns.

Importantly, the proposed rules regulate not only what information covered businesses may *collect*, but also what they may *infer* from information they have already collected. The regulation of inferences is a restriction on thought rather than a restriction on data processing. The Supreme Court has held that the "right to speak" encompasses the right to decide how "the information" one "possesses" "might be used or disseminated."[29] The proposed rules do not allow covered businesses this necessary discretion.

A blanket ban on personalized recommendations for minors is also misguided from a policy standpoint, and will make minors less safe online. Such systems perform many useful functions, including helping users discover relevant information, creators, communities, businesses, and safety resources. Personalized recommendations can also be an important part of trust and safety systems. Services use automated systems to detect spam, scams, abuse, potentially harmful material, and other content that users may not want to encounter. Algorithmic feeds can limit the spread of such harmful content more easily than reverse-chronological feeds.

18. Discuss how covered businesses currently determine age for compliance with other federal and state laws that require it.

COPPA is the main federal law regulating children's online privacy, and applies to providers "with actual knowledge that [personal] information was collected from a child."[30] Covered businesses have many sources of guidance on how to comply with this standard. While COPPA's statutory text does not further define the term "actual knowledge," the Federal Trade Commission (FTC) has issued guidance on this point. According to the FTC, "an operator has actual knowledge of a user's age if the site or service asks for — and receives — information

[28] 144 S. Ct. 2383, 2408 (2024).
[29] *Sorrel v. IMS Health, Inc.*, 564 U.S. 552, 568 (2011) (cleaned up).
[30] 15 U.S.C. § 6501(4)(B) (1998).

from the user that allows it to determine the person's age,"[31] e.g., by asking for a user's date of birth. Actual knowledge can also be satisfied through age-adjacent requests which provide operators with sufficient notice of a user's age. For example, questions that ask an individual's grade in school or what school they attend may satisfy actual knowledge under COPPA. FTC consent decrees have provided further guidance,[32] as have federal courts.[33]

This combination of underlying federal law, regulatory guidance, FTC enforcement actions, and judicial interpretation provides operators with many tools for understanding compliance requirements.[34] Conversely, as noted above, there is no established framework for determining which information a "covered business collects, processes, or infers" would indicate that a user is a minor.

While several states have sought to exceed the self-attestation requirement and institute age verification mandates, courts have been skeptical of their constitutionality. Several federal courts have held that laws requiring age verification and parental consent for social media sites violate the First Amendment's guarantee of free speech. The Supreme Court has repeatedly ruled that the First Amendment applies to teens as well as adults, holding that "[m]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them."[35] The Court has further held that "to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights."[36] Forcing covered operators to adopt age verification contradicts this ruling, foreclosing a wide range of protected speech for a population clearly entitled to access it. Such laws, in the Court's words, "do not enforce parental authority over children's speech . . . ; they impose *governmental* authority, subject only to a parental veto."[37] For these reasons, a wide array of lower courts have held that the First Amendment does not permit states to require age verification or parental consent to access protected speech as well.[38]

Implementing a statewide mandate with similar consequences in Vermont would cause similar constitutional problems. To avoid these problems, the AGO should continue to hold covered operators to the actual knowledge standard set forth in VAADCA.

19. Discuss how effective current federal and state age assurance requirements, such as state gambling laws, are in ensuring age accuracy.

[31] "Children's Online Privacy Protection Rule: Not Just for Kids' Sites," F.T.C. (May 2026), https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-not-just-kids-sites#when
[32] *See, e.g.*, *FTC v. Google*, No. 1:19-cv-02642 (D.D.C. Sept. 4, 2019); *United States v. Musical.ly*, No. 2:19-cv-01439 (C.D. Cal. Mar. 27, 2019).
[33] *See, e.g.*, *New Mexico v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1129 (D.N.M. 2020).
[34] *See also* Lieberfeld, *supra* note 20.
[35] *See, e.g.*, *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-13 (1975); *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 794 (2011).
[36] *Packingham v. North Carolina*, 582 U.S. 98, 108 (2017).
[37] *Brown*, 564 U.S. at 795 n. 3.
[38] *See, e.g.*, *NetChoice v. Hilgers*, No. 4:26-CV-3149, 2026 WL 1850018 (D. Neb. June 27, 2026); *NetChoice v. Jones*, 822 F. Supp. 3d 656 (E.D. Va. 2026); *NetChoice v. Murrill*, 812 F. Supp. 3d 594 (M.D. La. 2025); *NetChoice v. Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 (W.D. Ark. Mar. 31, 2025); *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024).

When states attempt to force online service providers to verify users' ages rather than permit age assurance, numerous problems arise. Many users will be above the age threshold but lack the required proof (such as a driver's license). Additionally, age estimation tools like face scans are prone to both false negatives and false positives.[39] Furthermore, similar age restrictions have been only marginally effective, reducing use of the restricted website by only 10-25 percent among the intended groups, with much of the lost traffic redirected to un-gated websites providing similar content.[40] The limited effectiveness of these measures should be weighed against their substantial consequences for privacy, competition, and access to protected speech. CCIA therefore again recommends replacing the "has reason to know" standard with an actual knowledge standard, as mandated by VAADCA.

20. Discuss the important elements of an age assurance method.

Age assurance is a complex topic and there is no unique and generally applicable solution with services opting for different approaches based on factors such as type of service, target audience, calculation and perception of the risks, privacy and security expectations of users, or economic feasibility, among others.[41]

Relying on industry's best practices and examining their accuracy and impact is a necessary first step. Established industry standards can provide great value in implementing the listed principles. Further, there is a need to guarantee operational capacity for adequate enforcement, allowing the industry to layer and combine different approaches when it comes to age assurance, in order to appropriately target the risks within the different parts of an online service.

21. Discuss the key challenges to an effective age assurance method.

Privacy concerns and technological limitations are among the foremost challenges in creating effective age assurance. Demanding precise age verification often requires collecting more sensitive personal data, such as government IDs or facial scans. This creates larger data pools, particularly attractive for malicious actors and which raise significant privacy concerns for all users, including minors themselves. CCIA recommends avoiding requirements that inadvertently lead to greater data collection than necessary.

Additionally, many age assurance technologies are not consistently effective or accurate across all demographics. This leads to high numbers of false positives, potentially denying adults access to legitimate services, and may even enhance discrimination against certain groups. In this context, CCIA warns against relying on technology that is not yet fully mature, which can create more problems than it solves.

---

[39] Hanaoka et al., *supra* note 27. For a summary of recent literature on various age assurance methods, *see* Trevor Wagener, *App Store Age Verification: Popular in Principle, Unworkable in Practice*, CCIA (Oct. 21, 2025), https://ccianet.org/articles/app-store-age-verification-popular-in-principle-unworkable-in-practice/.
[40] *See, e.g.*, Matthew Brown et. al., *Can Online Activity Be Regulated? Evidence from Adult Websites* (Aug. 4, 2026), https://mattbrownecon.github.io/assets/papers/ageverification/ageverification.pdf; Leonardo Bursztyn et al., Why Bans Fail: Tipping Points and Australia's Social Media Ban, U. Chi. (Apr. 27, 2026), https://home.uchicago.edu/bursztyn/WhyBansFail.pdf.
[41] *Age Assurance*, *supra* note 26.

22. List and discuss the types of age-assurance methods that are commercially reasonable and technically feasible.

While more stringent methods will be appropriate in certain circumstances, covered businesses should be given the option to rely on user self-attestation to ensure equitable enforcement. If self-attestation is not an option, determining whether a given age assurance method is "commercially reasonable and technically feasible" will almost certainly require case-by-case evaluations of granular details about digital services' designs, user behavior, and internal processes, balanced against common industry practices. Even issuing new regulatory guidance to resolve scoping ambiguities carries its own risks. Agency interpretations are inherently subject to change across administrations, particularly in an area as politically salient as online safety. This dynamic would increase the likelihood of inconsistent enforcement and undermine the stability that clear, durable legislative scoping provides.[42] Explicitly allowing covered businesses to rely on user-self-attestation avoids these problems.

23. Discuss how much the different types of age assurance methods cost and how cost is assessed.

While self-attestation frameworks can be implemented with minimal cost, age estimation and verification are substantial expenses for digital services. Third-party age verification services can cost up to $50,000 to install, plus per-user fees, costing businesses an estimated $500,000 overall.[43] Costs to implement such systems in-house are far higher, often reaching $2 million.[44]

The price of an age verification system, however, represents only part of the overall expense. Collecting sensitive data from users, proactively screening it, and properly securing it is a cost-intensive barrier to entry for smaller businesses.[45] ID requirements also deter customers and can cut businesses' conversion rates by half.[46] Furthermore, moving sensitive data across different platforms increases its vulnerability to hackers.

Startups are especially vulnerable to data breaches, as they more often need to rely on third-party vendors due to the lower up-front costs. The financial consequences of such breaches can be devastating for startups. The average cost of a data breach in 2025 was $160 per record, or $4.44 million per breach, enough to bankrupt many small companies.[47] Consequently, over 60 percent of startups close after being hacked.[48] For these reasons, the

[42] *See, e.g.*, Lieberfeld, *supra* note 20.
[43] *More Than Just a Number: How Determining User Age Impacts Startups*, Engine, 2 (last updated Aug. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[44] *Id.*
[45] Lieberfeld, *supra* note 20.
[46] *More Than Just a Number*, *supra* note 43, at 6.
[47] *Cost of a Data Breach Report*, IBM (2025), https://www.ibm.com/reports/data-breach.
[48] Robert Johnson III, *60 Percent Of Small Companies Close Within 6 Months Of Being Hacked*, Cybercrime (Jan. 19, 2023), https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.

above DTSP report found that "smaller companies may not be able to sustain their business" if forced to verify user ages.[49]

24. Discuss information the AGO should consider for purposes of "commercially reasonable and technically feasible" concerning the size of a covered business for age assurance methods.

Vermont should allow businesses to implement age assurance measures that are most appropriate to the types of data they process. A business should not be required to collect data it cannot properly secure. Accordingly, regulations should align with existing standards, such as those set forth by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). This will help businesses leverage the best existing security measures for age assurance data while avoiding duplicative compliance requirements that undermine efficiency. Such requirements should be general rather than prescriptive, requiring that businesses' security controls be reasonable and appropriate to the type, amount, and sensitivity of the information they process. This approach aligns with most existing laws and gives businesses the needed flexibility to combat security risks specific to their operations. Prescriptive requirements to institute specific security measures, by contrast, risk becoming obsolete as cyber threats evolve, imposing compliance burdens without enhancing security.

25. Discuss financial resources the AGO should consider in determining what is commercially reasonable and technically feasible for a covered business regarding age assurance methods.

While a business's financial resources are generally proportional to its ability to securely store sensitive information, there is no exact relationship between the two. As noted above, the "commercially reasonable and technically feasible" framework will inherently lead to inconsistent enforcement if self-attestation is not an option for users. The proposed rules should reflect this dynamic.

26. List and discuss technical capabilities the AGO should consider in determining what is commercially reasonable and technically feasible for a covered business regarding age assurance methods.

The AGO should consider adopting common industry frameworks for age assurance, such as those published by DTSP and ISO, as safe harbors that covered businesses can rely on to ensure compliance, as discussed below (see response to Question 30).[50] This will help ensure that covered businesses can know they are in compliance, and allows businesses to match their security practices to the type and amount of data they process. Consumer facing digital services have already built considerable consensus around mitigating content- and conduct-related risks to users and other parties. Most of the leading firms in the industry have

[49] *Age Assurance*, *supra* note 26.
[50] *See* ISO/IEC 25389:2025, *Information technology — The safe framework* (Edition 1, June 2025), https://www.iso.org/standard/90106.html; *Age Assurance*, *supra* note 26.

committed to meet best practice standards for online safety which are embedded in a recently published 2025 international standard.[51]

27. Discuss the impact using age assurance methods would have on the safety, utility, and experience of Vermonters using an online service.

Methods such as age verification that require Vermonters to share sensitive personal information substantially undermine privacy and security. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[52] Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[53] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[54]

28. Discuss what is considered an appropriate review process for an age appeal and whether the AGO should adopt certain elements, features, or steps for an appeal.

An appeals process should enable users to submit good-faith requests to change their age determination. However, allowing unlimited appeals allows malicious actors to spam covered businesses with fraudulent requests. Covered businesses would then have to divert resources away from bona fide requests in order to answer endless appeals. VDPOSA recognized this need by allowing operators the ability to ignore age appeals they believe to be fraudulent.[55] CCIA therefore recommends requiring covered operators to "provide a clear, accessible, and meaningful appeals process where appropriate, which shall be disclosed prior to the use of the service and in language that is easily understandable" rather than the proposed requirement to provide this process "for any age-related determination."[56]

29. Discuss the types of transparency measures that would help to increase consumer trust in an age assurance method.

When studying public trust of age assurance measures, a crucial pattern emerges: public support for protecting children online does not translate to willingness to upload IDs or face scans, or trust in common age assurance methods.[57] Utah State University's recent national

---

[51] *Id.*
[52] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *Principle (c): Data Minimisation,* U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.
[53] Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.
[54] Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.
[55] 9 V.S.A. § 2415d(c)(4)(C) (2026).
[56] "Age Assurance Privacy," *supra* note 2, at 10.
[57] Wagener, *supra* note 39.

survey showed two-thirds of Americans are not comfortable sharing a government ID with social media companies to verify their age, and nearly 70% are not comfortable sharing their child's ID.[58] A Carnegie Mellon University study showed that 52% were willing to undergo AI-based facial analysis, just 22-28% of participants were willing to upload their IDs for an age check, and just 17% were willing to accept a brief recording to prove they were human.[59] Similar findings have been demonstrated abroad: In the wake of the UK Online Safety Act rollout, Ipsos found public support for age checks in principle, but far less willingness to participate in common age assurance methods: only 19% would provide proof of age on dating apps, 37% for social media, and 38% for messaging services.[60] Such mandates would force Vermonters to choose between providing government IDs and face scans and accepting the associated data security risks, or losing access to online services that are critical for information, communication, and free expression.

30. Discuss whether a certification model like the Secretary of State's data broker registry would be sufficient for covered businesses to assert they comply with AADC rules.

A certification model that covered businesses can use as a safe harbor is an excellent way to ensure high standards and legal consistency. Safe harbor provisions are important for fair and effective enforcement. Safe harbors (1) provide valuable predictability to both market actors and consumers, (2) enable speedier compliance, and (3) deter vexatious, meritless litigation if in fact parties other than the state are authorized to enforce the statute. When the AGO alleges noncompliance with a privacy or security obligation, businesses should therefore be allowed to use compliance with an established privacy framework like NIST and ISO as an affirmative defense against such allegations. Businesses should also receive advance notice of complaints and have the opportunity to cure violations before enforcement actions are brought, both to minimize costly enforcement actions and focus agency resources on large-scale and repeat offenders.

31. Discuss the methods that should be considered to ensure that the privacy of user data is preserved in any age assurance method.

Many provisions of the proposed rules undermine user privacy and should be removed. Aside from the constructive knowledge standard discussed above, the proposed rules require covered businesses to "not send any push notification to a covered minor between the hours of 12:00 a.m. and 6:00 a.m.," except for transactional, safety, or account-related purposes.[61] Such requirements inevitably require that covered operators track when it is nighttime in a

[58] Taylor Barkley, *Poll: Americans Don't Want to Share Their Photo ID to Tweet*, Utah St. U. (Feb. 1, 2023), https://www.thecgo.org/benchmark/poll-americans-dont-want-to-share-their-photo-id-to-tweet/.
[59] Yanzi Lin et al., *User (Non-)Compliance with Age Verification: Preliminary Evidence from a Deceptive Web Experiment*, Carnegie Mellon U. CyLab Sec. & Priv. Inst., https://www.cs.cmu.edu/~sscheffl/docs/2026/AgeVerif2026.pdf.
[60] Keiran Pedley, *Britons Back Online Safety Act's Age Checks, but Are Sceptical of Effectiveness and Unwilling to Share ID*, Ipsos (Aug. 17, 2025), https://www.ipsos.com/en-uk/britons-back-online-safety-acts-age-checks-are-sceptical-effectiveness-and-unwilling-share-id.
[61] "Prohibited Data and Design Practices," *supra* note 1, at 11.

device's location. This requirement therefore effectively mandates location-based tracking of minors' devices, thus undermining the privacy of the very population the bill is designed to protect. Requiring covered operators to track their users serves no benefit, particularly since covered operators regularly give users the option to turn off notifications themselves.

32. Discuss whether certain data minimization practices should be adopted for AADC rules and if so, what data minimization procedures could be deployed to ensure compliance with the AADC.

Data minimization is a critical component of data security. Businesses should not be forced to collect data that they do not have the resources to process and store securely. This principle forms the foundation of longstanding privacy guidelines from the Federal Privacy Council, UK Information Commissioner, and other leading privacy authorities.[62] However, as noted above, the AGO's creation of a new knowledge standard undercuts this principle, as it incentivizes covered businesses to collect more data than they otherwise would to minimize legal exposure. The proposed rules would make privacy-invasive practices such as age verification the surest way to demonstrate compliance.

33. Discuss whether covered businesses and processors should use previously collected data to determine user age and if so, the type of data that would be most advantageous.

Businesses should be permitted to use previously collected data as an age signal where appropriate. COPPA enforcement should provide guidance regarding what types of information may be used for such purposes.[63] For instance, the length of time a user has held an account can indicate a user's minimum age, as can information in a user's bio or answers to survey questions posed by the online service, such as what grade a user is in. The AGO should adopt COPPA's guidance on which pieces of data constitute knowledge of a user's age.

34. Discuss the types of age assurance methods that are interoperable and whether the AGO should consider certain types over others and why.

Mandatory interoperability interfaces should be avoided, as they undercut user privacy. In particular, widespread consumer privacy rights like data deletion become nearly impossible to implement under such conditions: once a third party possesses a user's data, ensuring its deletion is generally infeasible.

Moreover, a public-facing interface designed for the purpose of extracting user data significantly increases the risk of data breaches. A hacker or foreign adversary accessing such an interface could obtain data from many social media users across several sites. In other key industries such as healthcare, interoperability of records has significantly increased vulnerability to cyberattacks in recent years.[64]

---

[62] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, *supra* note 52; *Principle (c): Data Minimisation, supra* note 52.
[63] *See* Lieberfeld, *supra* note 20.
[64] *See, e.g.*, Lancer Gates, *Cyber Attacks on Interoperable Electronic Health Records: A Clear and Present Danger*, 121 Mo. Med. 6, 6-9 (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC10887471/.

Different companies have different security practices. Some encrypt data while others do not. Companies also retain different types of data for different periods of time, and are bound by different laws and regulations if they operate across multiple jurisdictions, as online services tend to do. Many also tailor their security practices to the specific types of data they process. Interoperability requirements undermine companies' ability to create the best security features for their specific data uses, which in turn undermines their users' safety.

While interoperability requirements might save consumers a modicum of time when setting up a profile on a new social media site, the potential time saved is not worth the security risks. Companies should be allowed to protect their users' information in the best way possible given the configuration of their own websites without needing to water down such practices to make user data accessible to other companies.

35. Discuss the most effective, secure, private, affordable, quick, and easy-to-use, commercially reasonable, and technically feasible methods for any form of age assurance online.

The most appropriate age assurance methods will depend on a business's financial resources and the types of data they process. Ironically, by prohibiting design practices "designed to increase the frequency, duration, or intensity of a covered minor's interaction with an online service, product, or feature," the proposed rules create more legal risks for companies that invest the most in youth online safety and consumer protection. Developing online safety features for minors requires gathering data about users' ages, which leads to increased liability. Security fixes, better user features, and even improved processes for removing spam or other malicious content could therefore create additional liabilities for businesses, and thus require them to invest in costly age assurance measures. By contrast, those who avoid such investments can escape these obligations, and with it, the broad liability that attaches. Regulations should reward investments in online safety rather than deter them by tying those investments to additional legal and compliance burdens.

36. List/discuss whether there is anything else important for the AGO to consider in adopting AADC rules.

In general, far more care must be taken to adhere to the statutory mandate. The proposed rules contain many instances where the AGO has exceeded its rulemaking authority. Besides the instances noted above, the ban on secondary data use is broader than the statute permits. VAADCA allows covered businesses to "use previously collected personal data of a covered minor" for a "purpose other than a purpose for which the personal data was collected" if "necessary to comply with any obligation under this chapter."[65] However, the proposed rules do not permit secondary data uses *even if* they are necessary to comply with other VAADCA obligations, directly contradicting the statute.[66] The phrase "necessary to comply with any obligation under this chapter" should therefore be added to subsection (a) of the "Secondary Use" section. Likewise, subsections (c) and (d) of this section should be removed, as they contain activities that are not inherently secondary uses, such as model training and

[65] 9 V.S.A. § 2449f(a)(2) (2026).
[66] "Prohibited Data and Design Practices," *supra* note 1, at 5.

recommendation improvements (these practices do not even necessarily require personal data).

Other key terms are overbroad and create compliance difficulties, often worsening users' experience in the process. For instance, the phrase "specific and contemporaneous" should be removed from the definition of "express and unambiguous request," as a user typically selects account settings assuming that they will apply until the user changes them. The phrase "specific and contemporaneous" may prevent covered businesses from carrying over minors' account settings into subsequent sessions. Similarly, the proposed rules define "monitoring" such that almost any covered businesses "monitors" its users merely by running a website. Nearly all websites collect clicks and navigation patterns. This definition should be narrowed to real-time, continuous monitoring to avoid constantly requiring businesses to signal their users.

Lastly, covered businesses will not have sufficient time to institute the necessary compliance measures. The proposed rules take effect within 60 days of the comment submission deadline. Given the multitude of new practices covered businesses might need to adopt to attain compliance, CCIA recommends allowing covered businesses at least 12 months after this deadline to attain compliance.

* * * * *

While we share concerns regarding the safety of young people online and the importance of data privacy, we encourage the AGO to resist advancing regulations that pose significant compliance, privacy, and constitutional concerns, and to revise the proposed rules to ensure conformity with VAADCA.

We appreciate your consideration of these comments and welcome opportunities to provide additional feedback on this and other technology policy matters.

Sincerely,

Jesse Lieberfeld
Policy Counsel– Privacy, Security, & Emerging Technologies
Computer & Communications Industry Association